NETWORK INTRUSION DETECTION AND ANALYSIS SYSTEM AND METHOD

ABSTRACT OF THE DISCLOSURE

An intrusion detection and analysis system and method are disclosed. The system includes a data monitoring device comprising a capture engine operable to capture data passing through the network and configured to monitor network traffic, decode protocols, and analyze received data. The system further includes an intrusion detection device comprising a detection engine operable to perform intrusion detection on data provided by the data monitoring device. Application program interfaces are provided and configured to allow the intrusion detection device access to applications of the data monitoring device to perform intrusion detection. The system also includes memory for storing reference network information used by the intrusion detection device to determine if an intrusion has occurred